Allgemeine Software as a Service Bedingungen

der Ordio GmbH, Pilgrimstraße 6, 50674 Köln („Ordio“)

Stand April 2024

§ 1 Vertragsgegenstand

1.1 Gegenstand des Vertrags ist die Bereitstellung eines Zugangs zu den SaaS Services unter der Domain www.ordio.com sowie der angemessene Betrieb der SaaS Services zur Nutzung durch den Auftraggeber für die Laufzeit des Vertrags gegen Zahlung der vereinbarten Vergütung.

1.2 Dies ist eine Abonnementvereinbarung für den Zugang zum SaaS Service und dessen Nutzung. Der Auftraggeber erkennt an, dass er nur ein begrenztes Recht zur Nutzung des SaaS Services erhält und dass unabhängig von der Verwendung der Wörter „Kauf“, „Verkauf“ oder ähnlicher Begriffe im Rahmen dieser Vereinbarung oder sonstiger Kommunikation der Parteien keine Eigentumsrechte auf den Auftraggeber übertragen werden sollen. Der SaaS Service wird als Online-Produkt gehostet und ist über Web-Apps und Mobile Apps zugänglich. Dementsprechend erkennt der Auftraggeber an und stimmt zu, dass er kein Recht hat, eine Kopie der Software zu erhalten.

1.3 Nicht Gegenstand des Vertrags ist die Erbringung von Rechtsdienstleistungen. Allein der Auftraggeber ist dafür verantwortlich, sicherzustellen, dass er Gesetz und Recht in seinem Geschäftsbetrieb einhält.

1.4 Der Vertrag wird geschlossen, indem der Auftraggeber diese Allgemeinen Software as a Service Bedingungen („Bedingungen“) während des Registrierungsvorgangs akzeptiert. Akzeptiert der Auftraggeber diese Bedingungen nicht, kommt kein Vertrag über die Nutzung der SaaS Services zustande.

1.5 Der Vertrag setzt sich zusammen aus der Leistungsbeschreibung und der Vergütungsvereinbarung, die beide auf der Webseite www.ordio.com/preise dargestellt sind, sowie deren Bedingungen. Weiteren Regelungen werden nicht Teil dieses Vertrages, insbesondere keine Allgemeinen Geschäftsbedingungen des Auftraggebers, soweit sie in diesem Vertrag nicht ausdrücklich als Vertragsbestandteil aufgenommen worden sind. Dies gilt selbst dann, wenn der Auftraggeber auf seine Allgemeinen Geschäftsbedingungen verweist, der Auftragnehmer der Einbeziehung aber nicht widerspricht.

§ 2 Vertragsabschluss

2.1 Der Auftraggeber kann sich auf der Webseite www.ordio.de für einen Standort registrieren.

2.2 Der Auftraggeber hat bei der Bestellung eines kostenpflichtigen Abonnements die Möglichkeit, in der Bestellansicht seine Eingaben über die Funktion „bearbeiten“ zu ändern. Weitere Änderungen kann der Auftraggeber jederzeit in den „Einstellungen“ vornehmen.

2.3 Der Vertrag kann ausschließlich in deutscher Sprache geschlossen werden.

2.4 Diese AGB sowie die weiteren Vertragsbestimmungen können von dem Auftraggeber unmittelbar nach Vertragsschluss unter **www.ordio.com/agb** heruntergeladen und dauerhaft gespeichert werden.

§ 3 SaaS-Services

3.1 Der Auftragnehmer unternimmt angemessene Maßnahmen, um die Verfügbarkeit der SaaS Services gemäß Leistungsbeschreibung zu ermöglichen.

3.2 Während der Laufzeit des Vertrags wird der Auftragnehmer die SaaS Services während der Geschäftszeiten betreiben und die notwendigen Maßnahmen ergreifen, um den Betrieb aufrechtzuerhalten. Der Auftragnehmer gewährleistet, dass die SaaS Service 99,6-Prozent bezogen auf ein Kalenderjahr verfügbar sind. Verfügbar in diesem Sinne bedeutet, dass die SaaS Service am Routerausgang des Rechenzentrums des Auftragnehmers erreichbar sind und die wesentlichen Funktionen der SaaS Services ausgeübt werden können. Ausgenommen von dieser Verfügbarkeit sind Zeiträume der Nichtverfügbarkeit, (a) in denen der Auftraggeber geplante oder ungeplante Wartungsarbeiten an den SaaS Services durchführt, (b) die durch Umstände Höherer Gewalt verursacht wurden, (c) die auf

Umstände zurückzuführen sind, die der Auftragnehmer zu vertreten hat (z.B. Nichteinhaltung von Mitwirkungspflichten) und (d) die auf Umständen beruhen, die nicht vom Auftragnehmer zu vertreten sind. Wartungsarbeiten werden in der Regel zwischen 0:00 und 4:00 Uhr durchgeführt. Ein Ereignis höherer Gewalt liegt vor, wenn ein betriebsfremdes, von außen durch elementare Naturkräfte oder durch Handlungen dritter Personen herbeigeführtes Ereignis, das nach menschlicher Einsicht und Erfahrung unvorhersehbar ist, mit wirtschaftlich erträglichen Mitteln auch durch die äußerste nach der Sachlage vernünftigerweise zu erwartende Sorgfalt nicht verhütet oder unschädlich gemacht werden kann und auch nicht wegen seiner Häufigkeit von der betroffenen Partei in Kauf zu nehmen ist. Ereignisse höherer Gewalt können zum Beispiel sein: Feuer, Überschwemmung, Erdbeben, Naturelemente, Kriegshandlungen, Unruhen, Terrorismus, Pandemien, behördlichen Anordnungen, Revolutionen in einem Land, Streiks.

§ 4 Weiterentwicklung

4.1 Der Auftragnehmer behält sich das Recht vor, die SaaS Services in regelmäßigen oder unregelmäßigen Abständen grundlegend oder nur in Teilen zu überarbeiten und anzupassen, insbesondere technisch und funktional weiterzuentwickeln. Durch derartige Updates können weitere Leistungen hinzutreten, Leistungen abgeändert oder abgeschafft werden. Die Entscheidung, ob, innerhalb welchen Zeitraums und in welchem Umfang die SaaS Services weiterentwickelt werden, liegt beim Auftragnehmer. Der Auftragnehmer weist den Auftraggeber bei jedem Update auf die wesentlichen Änderungen hin. Der Auftraggeber erklärt sich bereits mit Vertragsschluss damit einverstanden, dass der Auftragnehmer derartige Updates durchführt.

4.2 Sollten die zusätzlichen Leistungen kostenpflichtig sein, besteht für den Auftraggeber die Möglichkeit, diese nicht in Anspruch zu nehmen.

§ 5 Support

5.1 Während der Laufzeit dieses Vertrags erbringt der Auftragnehmer die in der Leistungsbeschreibung beschriebenen Supportleistungen.

§ 6 Nutzungsrechte

6.1 Mit Einhaltung der Bestimmungen dieses Vertrags durch den Auftraggeber, insbesondere der fristgemäßen Zahlung, räumt der Auftragnehmer dem Auftraggeber das nicht- exklusive, nicht-übertragbare Recht ein, die SaaS Services innerhalb seines Geschäftsbetriebs innerhalb Deutschlands für die Laufzeit des Vertrags zu nutzen. Der Auftraggeber darf ausschließlich seinen Mitarbeitern gestatten, die SaaS Services zu nutzen; anderen Personen darf der Auftraggeber keinen Zugriff auf die SaaS Services gewähren. Zur Nutzung der SaaS Services ist jeder Mitarbeiter des Auftraggebers berechtigt, der über einen aktiven Account zu den SaaS Services verfügt. Aktiv ist ein Account, wenn sich der Mitarbeiter mindestens einmal in einem Kalendermonat bei den SaaS Services angemeldet hat.

6.2 Der Auftraggeber ist nicht berechtigt, die SaaS Services zu bearbeiten oder zu verändern, zu verbreiten oder öffentlich zugänglich zu machen, es sei denn, das Gesetz gestattet dies zwingend.

6.3 Die SaaS Services dürfen ausschließlich in Deutschland genutzt werden.

§ 7 Pflichten des Auftraggebers

7.1 Für einzelne Module können weitergehende Lizenzbeschränkungen (z.B. limitierte Anzahl zugelassener Mitarbeiter, limitierte Anzahl der Leistungsbeschreibung aufgeführt und vom Auftraggeber einzuhalten.

7.2 Der Auftraggeber stellt sicher, dass er die SaaS-Services nicht in einer Weise nutzt, die – möglicherweise – zu Unterbrechungen, Schäden oder Nicht-Verfügbarkeiten oder ähnlichem ungewünschten Verhalten der SaaS-Services oder Teilen davon führt.

7.3 Der Auftraggeber ist dafür verantwortlich, die notwendige Hardware, Internetverbindungen oder sonstige Dienstleistungen zu beziehen, zu implementieren und für die Laufzeit des Vertrages bereitzustellen, die notwendig sind, um sich zu den SaaS-Services zu verbinden und diese zu nutzen. Der Auftraggeber ist verpflichtet, die folgenden Systemanforderungen einzurichten und während der Laufzeit des Vertrags aufrechtzuerhalten:
- Browser etc. , Internetverbindung, optional Tablet/Smartphone (Unterstütze iOS und Android Version richtet sich nach der aktuellsten Expo-Version, zu finden unter: https://docs.expo.dev/versions/latest/)

7.4 Der Auftraggeber muss geeignete Maßnahmen zum Schutz der von ihm zur Nutzung der SaaS-Services eingesetzten Hard- und Software ergreifen, um die Sicherheit und Integrität der vom Auftragnehmer eingesetzten Systeme zu gewährleisten. Hierzu zählen unter anderem der aktuelle Einsatz von Betriebssystemen sowie der Einsatz aktueller Vorkehrungen zum Schutz der IT-Sicherheit (Virenschutzscanner, Firewall). Der Auftraggeber trägt dafür Sorge, dass diese Maßnahmen auch auf den Endgeräten, die von seinen Mitarbeitern eingesetzt werden, umgesetzt werden.

7.5 Der Auftraggeber setzt angemessene Maßnahmen ein, um zu verhindern, dass unberechtigte Personen die SaaS-Services nutzen können. Insbesondere wird der Auftraggeber angehalten seine Zugangsdaten für Dritte unzugänglich aufbewahren und geheim halten.

7.6 Der Auftraggeber ist nicht berechtigt, die SaaS-Services, insbesondere durch Uploads, E-Mails, Postings, Veröffentlichungen oder jede andere Art und Weise der Datenübertragung, zu verwenden, um

a) Material, das andere Personen herabsetzt, beleidigt oder anderweitig verletzten kann, zu verbreiten, falsches, herabsetzendes, beleidigendes oder obszönes Material zu verbreiten,
b) Persönlichkeitsrechte zu verletzen,
c) Straftaten zu begehen
d) Hass oder Rassismus zu fördern,
e) belästigendes Material, Massenbenachrichtigungen oder ähnliches durchzuführen,
f) Rechtsverletzungen zu begehen.

7.7 Der Auftraggeber garantiert, dass sowohl der Auftraggeber als auch die Nutzer die SaaS-Services in Übereinstimmung mit diesem Vertrag und den geltenden Gesetzen nutzen.

7.8 Der Auftragnehmer behält sich das Recht vor, Inhalte zu löschen oder zu blockieren, die gegen die Bestimmungen dieses Vertrags oder die geltenden Gesetze verstoßen. In einem solchen Fall übernimmt der Auftragnehmer keine Haftung gegenüber dem Auftraggeber. Der Auftraggeber wird alle Ansprüche abwehren und den Auftragnehmer von allen Ansprüchen freistellen, die im Zusammenhang mit der Verletzung von Pflichten des Auftraggebers aus diesem Vertrag stehen.

7.9 Mithilfe der SaaS Service können Personen, die die SaaS Services nutzen, unter- einander Verträge schließen. Der Auftraggeber tritt in eigenem Namen und in eigener Verantwortung gegenüber Dritten auf. Für das Rechtsverhältnis mit diesen Dritten ist ausschließlich der Auftraggeber verantwortlich.

§ 8 Vergütung

8.1 Für die Bereitstellung der SaaS Services verpflichtet sich der Auftraggeber zur Zahlung der auf der Webseite www.ordio.com zum Zeitpunkt des Vertragsschlusses aufgeführten Vergütung. Soweit in der Vergütungsvereinbarung auf der Webseite www.ordio.com oder individuell zwischen den Parteien vereinbart, zahlt der Auftraggeber dem Auftragnehmer für jeden Standort, den er über die SaaS-Services verwaltet, eine monatliche Vergütung. Die Höhe der Vergütung ist pro Modul und Standort festgelegt und kann unter www.ordio.com eingesehen werden. Pro Standort dürfen die auf der Webseite angegebene Höchstzahl von Mitarbeitern verwaltet werden, solange zwischen den Parteien nicht etwas anderes vereinbart wurde. Für diese Standorte schuldet der Auftraggeber die vereinbarte Vergütung.

8.2 Dem Auftraggeber steht es frei, die Nutzung der SaaS-Services für einen bestimmten Zeitraum kostenfrei bereitzustellen, damit der Auftragnehmer die SaaS-Services testen kann. Mit Ablauf dieses Zeitraums muss der Auftraggeber entweder eine Vergütung entrichten oder die Nutzung der SaaS-Services einstellen.

8.3 Alle Beträge verstehen sich zuzüglich der zum Zeitpunkt der Rechnungsstellung gültigen Umsatzsteuer, soweit diese anfällt.

8.4 Der Auftragnehmer stellt Rechnungen monatlich.

8.5 Die Rechnung ist sofort fällig. Abzüge (Skonto etc.) sind nicht zulässig. Der Auftraggeber kann wählen, über welchen vom Auftragnehmer auf der Webseite angebotenen Zahlungsdienst er die Vergütung an den Auftragnehmer bezahlen möchte.

8.6 Sollte die vorstehende Zahlungsvereinbarung nicht eingehalten werden und auch trotz Mahnung kein Zahlungseingang zu verzeichnen sein, ist der Auftragnehmer berechtigt, den Auftraggeber von der Nutzung der Software auszuschließen.

8.7 Haben der Auftraggeber und der Auftragnehmer vereinbart, dass die SaaS Services (zunächst) kostenfrei erbracht werden, steht es dem Auftragnehmer frei,

eine Vergütung für die SaaS Services zu verlangen. Macht der Auftragnehmer dieses Recht geltend, wird er den Auftraggeber schriftlich darauf hinweisen, dass zukünftig eine Vergütung fällig wird. Der Auftragnehmer wird dem Auftraggeber dies mindesten drei (3) Monate vor Wirksamwerden mitteilen. Dem Auftraggeber steht es frei, diesen Vertrag sodann zu kündigen. Kündigt der Auftraggeber den Vertrag nicht, gilt die Vergütung mit Ablauf der Frist als vereinbart. Der Auftragnehmer wird den Auftraggeber in der Information darauf hinweisen.

§ 9 Vertragslaufzeit und Kündigung

9.1 Dieser Vertrag tritt in Kraft, wenn sich der Auftraggeber auf der Webseite registriert und der Vertrag zwischen dem Auftraggeber und dem Auftragnehmer zustande gekommen ist.

9.2 Abhängig von der Auswahl des Auftraggebers hat der Vertrag grundsätzlich eine Vertragslaufzeit von einem (1) Monat oder von zwölf (12) Monaten und verlängert sich am Ende der aktuellen Vertragslaufzeit erneut um die jeweils ausgewählte Vertragslaufzeit, wenn der Vertrag nicht vorab mit einer Frist von einer (1) Woche zum Ende der jeweiligen Vertragslaufzeit durch eine Partei gekündigt wird. Die Vertragslaufzeit von einem (1) bzw. von zwölf (12) Monaten beginnt immer am ersten des auf den Tag des Vertragsschluss folgenden Monat. Dies hat zur Folge, dass die Zeit zwischen Vertragsschluss und dem Beginn der Vertragslaufzeit anteilig berechnet und der Vertragslaufzeit addiert wird. Die anteiligen Kosten trägt der Auftraggeber.

9.3 Hat der Auftraggeber einzelne Module gebucht, kann der Auftraggeber jeweils mit einer Frist von einer (1) Woche zum Ende eines Kalendermonats die Nutzung eines Moduls kündigen. Dem Auftragnehmer steht dasselbe Recht hinsichtlich einzelner Module zu.

9.4 Das Recht der Kündigung der Vereinbarung aus wichtigem Grund bleibt unberührt.

9.5 Für den Fall, dass im Rahmen des § 3 3.1. dieses Vertrages Leistungen ersatzlos wegfallen, die für den Auftraggeber von wesentlichem Interesse und seinerzeit ausschlaggebend für den Vertragsschluss waren, steht diesem ein außerordentliches Kündigungsrecht zu.

9.6 Die Kündigung kann per Brief, per E-Mail oder über die SaaS Services erfolgen.

9.7 Mit Ablauf oder Kündigung dieses Vertrages erlöschen die Nutzungsrechte des Auftraggebers, und er muss unverzüglich die Nutzung des/der betreffenden Dienste(s) einstellen, jegliche Dokumentation, Passwörter und/oder Zugangscodes und alle anderen vertraulichen Informationen im Zusammenhang mit dem Auftragnehmer sowie den dem SaaS Service löschen (oder auf Anfrage von des Auftragnehmers zurückzugeben). Es erlischt das Recht des Auftraggebers, auf Daten im innerhalb des SaaS Service zuzugreifen und der Auftragnehmer kann die Daten nach dreißig (30) Tagen ab dem Datum der Kündigung unwiderruflich löschen

§ 10 Haftung

10.1 Der Auftragnehmer haftet dem Auftraggeber für alle Schadens-, Aufwendungs-, Wertersatz- oder Rückerstattungsansprüche (nachfolgend „Schäden“) innerhalb eines zwölf Monats Zeitraums höchstens in der Höhe, die der vom Auftraggeber in den vorhergehenden zwölf Monaten an den Auftragnehmer bezahlten Vergütung entspricht.

10.2 Die Haftung des Auftragnehmers für entgangenen Gewinn, entgangene Geschäftschancen, Reputationsverluste oder eine Minderung des Firmenwerts ist ausgeschlossen.

10.3 Die vorstehenden Haftungsbeschränkungen gelten nicht für

a) Schäden aus der Verletzung des Lebens, des Körpers, der Gesundheit;
b) bei Vorsatz oder grober Fahrlässigkeit;
c) im Rahmen übernommener Garantien des Auftragnehmers;
d) in Fällen von Arglist und
e) soweit eine solche Haftungsbeschränkung bzw. ein Haftungsausschluss nach dem geltenden Recht, unter anderem dem Produkthaftungsgesetz, nicht zulässig ist.

10.4 Die verschuldensunabhängige Haftung für vor Vertragsbeginn entstandene Schäden und Aufwendungen ist ausgeschlossen (§ 536a BGB). Der Auftragnehmer haftet insoweit verschuldensabhängig nach Maßgabe dieser Ziffer.

§ 11 Freistellung

11.1 Der Auftragnehmer stellt den Auftraggeber im Rahmen der vereinbarten Haftungsgrenzen von Ansprüchen frei, die von Dritten innerhalb des Nutzungsgebiets, in dem der Auftraggeber die Software nutzen darf, geltend gemacht werden und die auf der Verletzung von Immaterialgüterrechten des

Dritten wegen einer nach dieser Vereinbarung bestimmungsgemäßen und erlaubten Nutzung der SaaS Services durch den Auftraggeber stehen. Dies gilt jedoch nicht, soweit ein solcher Anspruch, dadurch verursacht wurde, dass die SaaS Services durch den Auftraggeber (oder die Nutzer) nicht vertragsgemäß genutzt wurden.

11.2 Wird die Software (ggf. in Teilen) Gegenstand von Ansprüchen eines Dritten wegen der Verletzung von Immaterialgüterrechten, ist der Auftragnehmer auf seine Kosten und gemäß seiner Wahl berechtigt:

a) die SaaS Services oder Teile davon durch gleich- wertige zu ersetzen, die keine Immaterialgüterrechte Dritter verletzen, die jedoch im Wesentlichen die vereinbarte Beschaffenheit aufweisen,
b) die SaaS Services oder Teile davon zu verändern, damit sie keine Immaterialgüterrechte Dritter verletzen, ohne die vertragsgemäße Möglichkeit der Nutzung der SaaS Services durch den Auftraggeber wesentlich zu beeinträchtigen; oder
c) die erforderlichen Nutzungsrechte an den SaaS Services ohne Mehrkosten für den Auftraggeber zu beschaffen. Wenn die vorstehenden Alternativen für den Auftragnehmer unzumutbar sind, ist der Auftragnehmer berechtigt, diesen Vertrag außerordentlich zu kündigen und dem Auftraggeber die Vergütung zu erstatten, die dieser bereits für die Zeit nach Wirksamwerden der Kündigung gezahlt hat.
d) Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen, Verbindlichkeiten, Kosten (einschließlich angemessener Rechtsverfolgungskosten) frei, die im Zusammenhang mit der Beeinträchtigung von Rechten, insbesondere von Schutzrechten, Dritter wegen der zugelassenen Nutzung von Mitarbeiterdaten im Einklang mit dieser Vereinbarung stehen.

11.3 Werden Ansprüche von Dritten geltend gemacht, werden sich die Parteien hierüber unverzüglich unterrichten. Der freistellenden Partei obliegt die Abwehr derartiger Ansprüche und die Streitbeilegungen, es sei denn, eine solche Streitbeilegung erfordert keine finanziellen Verpflichtungen, kein Schuldanerkenntnis und keine Haftungsübernahme für die jeweils andere Partei. Die Parteien werden die Abwehr derartiger Ansprüche in enger Abstimmung koordinieren und sich mit wirtschaftlich zumutbaren Maßnahmen unterstützen.

§ 12 Datenschutz

12.1 Soweit der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, gelten die Bestimmungen des beigefügten Auftragsverarbeitungsvertrags zwischen Auftraggeber und Auftragnehmer (Anlage 1 – Auftragsverarbeitungsvertrag).

§ 13 Vertraulichkeit

13.1 Soweit nicht anders in dieser Ziffer bestimmt, verpflichtet sich jede Partei (nachfolgend Empfänger) hinsichtlich vertraulicher Informationen der jeweils offenlegenden Partei (nachfolgend Offenlegender)

a) die vertraulichen Informationen geheim und vertraulich zu behandeln;
b) die vertraulichen Informationen nicht ohne vorherige schriftliche Erlaubnis des Offenlegenden zu offenbaren; und
c) zumindest die gleiche Sorgfalt anzuwenden, die der Empfänger selbst zum Schutz seiner vertraulichen Informationen anwendet, jedenfalls die verkehrs-erforderliche Sorgfalt für den Schutz solcher vertraulichen Informationen.

13.2 Die Bezeichnung “Vertrauliche Informationen” umfasst sämtliche Informationen des Offenlegenden:

a) die als “vertraulich” gekennzeichnet sind,

b) die - mündlich, schriftlich, elektronisch oder in anderer Form - zum Zeitpunkt der Offenlegung oder Kenntnisnahme aufgrund der Umstände der Weitergabe oder ihrer Natur als vertraulich erkennbar sind. Vertrauliche Informationen sind nicht Informationen, die dem Empfänger nachweislich

- vor Offenbarung durch den Offenlegenden ohne Verstoß gegen diese Vereinbarung in rechtmäßiger Art und Weise bekannt oder öffentlich zugänglich waren;
- dem Empfänger bereits vor Auferlegung einer Vertraulichkeitsverpflichtung zugänglich gemacht worden sind;
- dem Empfänger von einem dazu berechtigten Dritten in rechtmäßiger Art

und Weise ohne Verletzung einer Vertraulichkeitsverpflichtung zugänglich gemacht worden sind.

13.3 Der Empfänger darf die vertraulichen Informationen weitergeben

a) an seine mit der Durchführung dieser Vereinbarung befassten Mitarbeiter und etwaige Subunternehmer;
b) an seine professionellen Berater und Wirtschaftsprüfer; und
c) soweit dies zwingend gesetzlich erforderlich ist; (für (a) – (c)) vorausgesetzt, der Empfänger gewährleistet, dass die weiteren Empfänger eine den Bestimmungen dieser Vertraulichkeitsverpflichtung entsprechende Verpflichtung zur Vertraulichkeit einhalten.
d) Bei Kündigung oder Beendigung dieser Vereinbarung ist der Empfänger verpflichtet, die vertraulichen Informationen unverzüglich an den Offenlegenden zurückzugeben und keine Vervielfältigungen hiervon zurückzuhalten sowie elektronisch gespeicherte vertrauliche Informationen zu löschen. Diese Verpflichtung zur Rückgabe oder Löschung von vertraulichen Informationen gilt nicht, solange und soweit der Empfänger gesetzlich verpflichtet ist, solche vertraulichen Informationen zurückzubehalten/zu speichern. Sie gilt ferner nicht, solange und soweit vertrauliche Informationen nur mit unverhältnismäßigem Aufwand aus Backup-Systemen entfernt werden können. In solchen Fällen wird der Empfänger die vertraulichen Informationen blockieren und gewährleisten, dass auf die vertraulichen Informationen nicht von Dritten abgerufen werden können.

§ 14 Sonstiges

14.1 Für diese Vereinbarung gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen vom 11. April 1980 über Verträge über den internationalen Warenkauf (CISG) sowie unter Ausschluss der Verweisungsregelungen des deutschen internationalen Privatrechts in seiner jeweils gültigen Fassung.

14.2 Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Köln, Deutschland.

14.3 Sollte ein Teil dieses Vertrags ganz oder teilweise undurchsetzbar, nichtig oder unwirksam sein oder werden, bleiben die Wirksamkeit und Durchsetzbarkeit des Vertrages selbst und der übrigen vertraglichen Bestimmungen davon unberührt. Die Parteien werden sich bemühen, undurchsetzbare, nichtige oder unwirksame Bestimmungen durch diejenigen wirksamen und durchsetzbaren Bestimmungen zu ersetzen, die dem wirtschaftlichen Zweck der Parteien am nächsten kommen. Bis dahin gilt das Gesetz.

14.4 Zustimmungen und Genehmigungen einer Partei dürfen nicht unangemessen zurückgehalten oder verzögert werden. Solche Zustimmungen und Genehmigungen gelten nicht als Befreiung einer Partei von ihren Verpflichtungen oder Verzicht auf ihre Rechte aus dieser Vereinbarung.

14.5 Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der elektronischen Form.

Auftragsverarbeitungsvertrag (Stand Februar 2024)

im Sinne des Art. 28 Abs. 3 Datenschutzverordnung (DSGVO)

zwischen

_____

als Verantwortlicher (nachfolgend „**Verantwortlicher**“),

und

Ordio GmbH, Pilgrimstraße 6, 50674 Köln, Deutschland

als Auftragsverarbeiter (nachfolgend „**Auftragsverarbeiter**“,

Verantwortlicher und Auftragsverarbeiter gemeinsam die “**Parteien**”)

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „**Hauptvertrag**“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die “**Vereinbarung**”), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

1.1 Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

1.2 Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.3 Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**Betroffener**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4 Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrische Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

1.5 Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung,

Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.6 Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

2.1 Auftragsverarbeiter und Verantwortlicher haben einen Vertrag über die Bereitstellung und Nutzung der SaaS Services (nachfolgend. „Leistungen“) unter der Domain www.ordio.com (nachfolgend: „Hauptvertrag“ genannt) geschlossen. Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

2.2 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2.3 Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

2.4 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

3.1 Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.2 Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

3.3 Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3.4 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen, Drittland

4.1 Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

4.2 Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt.

4.3 Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

5.1 Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2 Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 4** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.3 Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "**Mitarbeiter**"), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

5.4 Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Informationspflichten des Auftragsverarbeiters

6.1 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

6.2 Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

6.3 Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

6.4 Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 7 Kontrollrechte des Verantwortlichen

7.1 Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Kontrollen sind rechtzeitig im Vorfeld anzumelden und erfolgen während der Geschäftszeiten des Auftragsverarbeiter. Der Verantwortliche

wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

7.2 Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

7.3 Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Einsatz von Dienstleistern

8.1 Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 3** genannten Dienstleister (nachfolgend "**Unterauftragsverarbeiter**") durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

8.2 Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

8.3 Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von 2 Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht dem Auftragsverarbeiter ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

8.4 Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

8.5 Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

§ 9 Anfragen und Rechte Betroffener

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

9.2 Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Haftung

10.1 Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter allein der Verantwortliche gegenüber dem Betroffenen verantwortlich.

10.2 Der Auftragsverarbeiter haftet für Schäden unbeschränkt, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragsverarbeiters, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

10.3 Für fahrlässiges Verhalten haftet der Auftragsverarbeiter nur bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertraut und vertrauen darf, jedoch beschränkt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragsverarbeiters - auch für seine Erfüllungs- und Verrichtungsgehilfen - ausgeschlossen.

10.4 Die Haftungsbegrenzung gemäß § 10.3 gilt nicht für Schadensersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit oder aus der Übernahme einer Garantie.

§ 11 Beendigung des Hauptvertrags

11.1 Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

11.2 Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

11.3 Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

12.1 Soweit der Auftragsverarbeiter Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

12.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

12.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

12.4 Diese Vereinbarung unterliegt deutschem Recht.

Verantwortlicher	**Auftragsverarbeiter**
Name:	Name:
_____	David_Keuenhof,_Ordio_GmbH_____
Position:	Position:
_____	CEO_____
Datum:	Datum:
_____	_____
Unterschrift:	Unterschrift:
_____	_____

Anlage 1 – Beschreibung der Daten/Datenkategorie

- Logindaten
- Name
- Rolle
- Schichtpläne
- Zeiterfassungsdaten
- Checkliste
- Verfügbarkeiten
- Inhalte aus hochgeladenen Dokumenten
- Daten in der Personalakte
- Meta- und Kommunikationsdaten (wie IP-Adressen)
- Daten zur Verifizierung
- Angaben zu Supportanfragen

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

- Mitarbeiter:innen des Verantwortlichen

Anlage 3 - Verzeichnis von Unterauftragsverarbeiter (Stand April 2024)

Name	Funktion	Hosting in	Anschrift
Hetzner	Hosting der Website	EU	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen in der EU
Sentry	Überwachung von Anwendungen und Fehlerverfolgung in Anwendungen oder auf Websites	USA	Functional Software, Inc., 132 Hawthorne Street San Francisco, CA 94107, USA
GitLab	Kollaboration bei der Arbeit, Versionsverwaltung für Softwareentwicklungen und Quellcodeverwaltung	USA	GitLab, Inc., 268 Bush St Ste 350, San Francisco, CA 94104, USA
Hubspot	Kundendialog und Kundensupport	EU	HubSpot, Inc., 25 1st Street Cambridge, MA 0214, USA

Anlage 4 - Technische und organisatorische Maßnahmen (Stand April 2024)

1 Einleitung

Dieses Dokument fasst die vom Verantwortlichen getroffenen technische und organisatorische Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Verantwortliche personenbezogene Daten schützt. Das Dokument hat den Zweck, den Verantwortlichen bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

2 Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) insb. durch

2.1 Zugriffskontrolle (z.B. Berechtigungskonzepte, Zugriffsprotokolle)

Angemessene Maßnahmen, die den Zugriff unautorisierter Personen auf die Datenverarbeitungssysteme verhindern, durch:

- Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts (Differenzierte Berechtigungen über Profile, Rollen, Transaktionen, Objekte, zeitliche Begrenzung) und der Zugriffsrechte sowie deren Überwachung und Protokollierung;
- Bereitstellung angemessener Funktionen zur Authentisierung;
- Aufzeichnung und Auswertung von Protokollen (erfolglose und erfolgreiche Authentifizierungsversuche);
- Verschließbarkeit der Einrichtungen zur Datenverarbeitung (Räume, Gebäude, Computerhardware und zugehöriges Equipment);
- Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden;
- Einsatz von Aktenvernichtern;
- Einsatz von Verschlüsselungsverfahren;

2.2 Zutrittskontrolle

Angemessene Maßnahmen zur Verhinderung des Zutritts unautorisierter Personen zum Datenverarbeitungsequipment, durch

- Zutrittskontrolle für Mitarbeiter und Dritte;
- Türsicherung (elektrische Türöffner, Ausweisleser, Fernsehmonitor, Empfang, usw.);
- Berechtigungsausweise;
- Schlüsselregelung;
- Sicherung des Gebäudes auch außerhalb der Arbeitszeit durch Alarmanlage Video- / Fernsehmonitor und/oder Werkschutz;
- Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde);
- Nutzung von Berechtigungsausweisen;
- Regelung für Firmenfremde;
- Nutzung von Besucherausweisen;

2.3 Zugangskontrolle (Kennwörter, Verschlüsselung von Datenträgern etc.)

Angemessene Maßnahmen, die sicherstellen, dass diejenigen, die bei der Datenverarbeitung eingesetzt werden, lediglich Zugang zu solchen Daten haben, die von ihrer jeweiligen Zugangsautorisierung abgedeckt sind, durch:

- Autorisierter Zutritt in Büroräumlichkeiten;
- Berechtigungskonzepte: Nur passwortgeschützte Zugriffe inkl. Rollenkonzepte in allen datenverarbeitenden und datenspeichernden Systemen;
- Zuordnung einzelner Clients und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen;

- Protokollierung und Auswertung der Dateibenutzung;
- Prüf-, Abstimm- und Kontrollsysteme;
- Programmprüfungs- und Freigabeverfahren;
- Verschlüsselung von Notebooks/Tablets;
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren;
- Nutzung von 2-Faktor-Authentifizierung;
- Firewalls;
- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit;

2.4 Pseudonymisierung und Verschlüsselung

Angemessene Maßnahmen, die eine Pseudonymisierung und Verschlüsselung der Daten umsetzen:

- RS265 Verschlüsselung in der Datenbank;

3 Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DSGVO) insb. durch

3.1 Weitergabekontrolle (z.B. Verschlüsselung, VPN)

Angemessene Maßnahmen, die bei einer weiteren Übermittlung der Daten (elektronisch oder auch Transport auf Datenträgern) sicherstellen, dass keine unbefugten Dritten die Daten lesen, löschen, ändern, kopieren durch:

- Verschlüsselung bei Datenübertragung (Netzwerkverschlüsselung, TLS, PGP);
- Protokollierung bei der Übermittlung von Daten;
- Zugriff für bestimmte autorisierte Benutzer;
- Gesonderter Verschluss vertraulicher Datenträger;
- Sicherheitsschränke;

3.2 Eingabekontrolle (z.B. Dokumentenmanagement, Protokollierung)

Der Auftragnehmer trägt dafür Sorge, dass nachträglich geprüft und festgestellt werden kann, ob und wann personenbezogene Daten in Datenverarbeitungssysteme eingegeben worden sind, durch:

- Einsatz von Protokollierungs- und Protokollauswertungssystemen;
- Verwendung von Logfiles;
- Anweisung an Mitarbeiter, nur nach Rücksprache Daten zu löschen;
- Verpflichtung auf das Datengeheimnis und zur Vertraulichkeit;

3.3 Auftragskontrolle

Die von dem Auftragnehmer verarbeiteten und genutzten Daten dürfen ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers verarbeitet werden. Dies wird sichergestellt durch:

- Eindeutige vertragliche Regelungen;
- Sorgfältige Auswahl des Auftragnehmers;
- Überprüfung der Einhaltung der vertraglichen Regelungen;

4 Sicherstellung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) insb. durch

4.1 Verfügbarkeitskontrolle (z.B. Backup-Strategie, Virenschutz, unterbrechungsfreie Stromversorgung, Notfallpläne etc.)

Angemessene Maßnahmen, die die Daten gegen zufällige Zerstörung oder Verlust schützen, durch:

- Backups gemäß Back-Up-Plan;
- Virenschutz/Firewalls;
- Spiegeln von Daten;
- Absicherung der Systeme gegen Ausfall der Datenbank, Service-Level-Agreements;

4.2 Trennungskontrolle

Angemessene Verfahren, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- Mandantentrennung;
- Funktionstrennung;
- Logische Trennung;
- Festlegung von Datenbankrechten;

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO) insb. durch

5.1 Datenschutz-Management

Angemessene Maßnahmen, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist

- Verwendung der heyData-Plattform zum Datenschutz-Management;
- Bestellung des Datenschutzbeauftragten heyData;
- Verpflichtung der Mitarbeiter auf das Datengeheimnis;
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz;
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO);

5.2 Incident Response Management

Angemessene Maßnahmen, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO);
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO);
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen;

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Angemessene Maßnahmen, die den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung tragen

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default";
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.